UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,303	08/30/2000	Douglas B. Moran	RECOP012	2514

21912 7590 11/12/2003

VAN PELT & YI LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
BAUM, RONALD	
ART UNIT	PAPER NUMBER
2131	7

DATE MAILED: 11/12/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

7

Office Action Summary	**Application No.** 09/651,303	**Applicant(s)** MORAN, DOUGLAS B.
	Examiner Ronald Baum	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) ☐ Notice of Informal Patent Application (PTO-152)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5 .	6) ☐ Other: .

DETAILED ACTION

1. Claims 1-23 are pending for examination.

2. Claims 1-23 are rejected.

Specification

3. The disclosure is objected to because of the following informalities: The attempt to incorporate subject matter into this application by reference to US patent applications only by a title (i.e., page 1, lines 9-12, "SYSTEM AND METHOD FOR DETECTING COMPUTER INTRUSIONS", and other locations on pages 1-2) is improper because reference to said documents is incomplete without more specific identification (i.e., actual US patent applications numbers).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-23 are rejected under 35 U.S.C. 102(b) as being anticipated by Maloney et al, U.S. Patent 6,269,447 B1.

4. As per claim 1 ; "A system for detecting intrusions [ABSTRACT, col. 1,lines 20-31,40-50, col. 2,lines 12-14,34-40, col. 3,lines 1-14, col. 12,lines 21-35], comprising: an analysis engine [col. 2,lines 41-47, col. 3,lines 28-32, col. 4,lines 43-50, col. 5,lines 54-62, col. 7,lines 7-

12]; and at least one sensor, configured to communicate with the analysis engine using at least one meta-protocol including a 4-tuple [figure 2 (meta data reference, and network addressing/database entry referencing parameters), col. 1,lines 54-col. 2,line 10, col. 2,lines 16-33,48-50('deriving generic structure' reference), col. 4,lines 15-22,34-37, col. 5,lines 24-28,39-52,63-67, col. 6,lines 38-44, col. 8,lines 27-34, col. 9,lines 24-30,47-50,54-58, col. 11,lines 47-col. 12,line 2].";

And further as per claim 22; "A method for detecting intrusions [This claim is the method of the apparatus (system) claim 1, and is rejected for the same reasons provided for the claim 1 rejection above], comprising the steps of- providing an analysis engine; providing at least one sensor; and defining a meta-protocol including a 4-tuple for communication between the analysis engine and the at least one sensor.".;

And further as per claim 23; "A computer program product for detecting intrusions on a host [This claim is the embodied in software method of the method claim 22, and is rejected for the same reasons provided for the claim 22 rejection above], the computer program product being embodied in a computer readable medium having machine readable code embodied therein for performing the steps of: providing an analysis engine; providing at least one sensor; and defining a meta-protocol including a 4-tuple for communication between the analysis engine and the at least one sensor.".

5. Claim 2 ***additionally recites*** the limitations that "The system as recited in claim 1, wherein the meta-protocol includes a data packet, and the data packet includes the 4-tuple. ". The teachings of Maloney et al (figure 2 (meta data reference, and network addressing/database entry referencing parameters)) suggest such limitations;

6. Claim 3 ***additionally recites*** the limitations that "The system as recited in claim 1, wherein the 4-tuple describes a data item.". The teachings of Maloney et al (figure 2 (meta data reference, and network addressing/database entry referencing parameters)) suggest such limitations;

7. Claim 4 ***additionally recites*** the limitations that "The system as recited in claim 3, wherein the 4-tuple comprises a semantic type, data type, data type size, and value of the data item.". The teachings of Maloney et al (figure 2 (meta data reference, and network addressing/database entry referencing parameters), and figure 4 (i.e., the address, password, user, etc., parameters represent the equivalent)) suggest such limitations;

8. Claim 5 ***additionally recites*** the limitations that "The system as recited in claim. 4, wherein the analysis engine is configured to use the data item to detect an intrusion.". The teachings of Maloney et al (ABSTRACT, col. 1,lines 20-31,40-50, col. 2,lines 12-14,34-40, col. 3,lines 1-14, col. 12,lines 21-35) suggest such limitations;

9. Claim 6 ***additionally recites*** the limitations that "The system as recited in claim. 1, wherein the at least one sensor is configured to communicate with the analysis engine using a plurality of meta-protocols.". The teachings of Maloney et al (figure 2 (meta data reference, and network addressing/database entry referencing parameters), col. 1,lines 54-col. 2,line 10, col. 2,lines 16-33,48-50('deriving generic structure' reference), col. 4,lines 15-22,34-37, col. 5,lines 24-28,39-52,63-67, col. 6,lines 38-44, col. 8,lines 27-34, col. 9,lines 24-30,47-50,54-58, col. 11,lines 47-col. 12,line 2) suggest such limitations;

10. Claim 7 ***additionally recites*** the limitations that "The system as recited in claims 6, wherein each of the plurality of meta-protocols includes a 4-tuple.". The teachings of Maloney

et al (figure 2 (meta data reference, and network addressing/database entry referencing parameters), col. 1,lines 54-col. 2,line 10, col. 2,lines 16-33,48-50('deriving generic structure' reference), col. 4,lines 15-22,34-37, col. 5,lines 24-28,39-52,63-67, col. 6,lines 38-44, col. 8,lines 27-34, col. 9,lines 24-30,47-50,54-58, col. 11,lines 47-col. 12,line 2) suggest such limitations;

11. Claim 8 ***additionally recites*** the limitations that "The system as recited in claim 6, wherein the analysis engine is configured to invoke the at least one sensor and specify a set of meta-protocols supported by the analysis engine, and wherein the at least one sensor is configured to select a meta-protocol from the set.". The teachings of Maloney et al (col. 8,lines 19-26, col. 5,lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (data and meta data levels), col. 8,lines 34-40, col. 9,lines 55-60) suggest such limitations;

12. Claim 9 ***additionally recites*** the limitations that "The system as recited in claim 8, wherein the set is a null set, and the at least one sensor is configured to use a default protocol.". The teachings of Maloney et al (col. 8,lines 19-26, col. 5,lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (data and meta data levels, including active, initialized, default (i.e., null set specified), and degraded states (i.e., figure 3, 'promiscuous mode' reference), col. 8,lines 34-40, col. 9,lines 55-60) suggest such limitations;

13. Claim 10 ***additionally recites*** the limitations that "The system as recited in claim 7, wherein the analysis engine is configured to specify a set of semantic codes representing data being requested by the analysis engine.". The teachings of Maloney et al (figure 2 (meta data reference, and network addressing/database entry referencing parameters), col. 1,lines 54-col.

2,line 10, col. 2,lines 16-33,48-50('deriving generic structure' reference), col. 4,lines 15-22,34-37, col. 5,lines 24-28,39-52,63-67, col. 6,lines 38-44, col. 8,lines 27-34, col. 9,lines 24-30,47-50,54-58, col. 11,lines 47-col. 12,line 2, figure 4 references to the various applications, and password types (i.e., FTP versus WWW versus POP3, etc.)) suggest such limitations;

14. Claim 11 ***additionally recites*** the limitations that "The system as recited in claim 10, wherein the at least one sensor is configured to supply data associated with the semantic codes, and wherein the at least one sensor further supplies data not associated with the semantic codes.". The teachings of Maloney et al (col. 8,lines 19-26, col. 5,lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (data and meta data levels, including active, initialized, default (i.e., null set specified), and degraded states (i.e., figure 3, 'promiscuous mode' reference would encompass allowing data transfer of specified and *non-specified types (i.e., semantic specification*) of data as per a given specified or selected (meta) protocol), col. 8,lines 34-40, col. 9,lines 8-14,55-60) suggest such limitations;

15. Claim 12 ***additionally recites*** the limitations that "The system as recited in claim 11, wherein the analysis engine is configured to disregard the data not associated with the semantic codes.". The teachings of Maloney et al (col. 8,lines 19-26, col. 5,lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (data and meta data levels, including active, initialized, default (i.e., null set specified), and degraded states (i.e., figure 3, 'promiscuous mode' reference would encompass allowing data transfer of specified and non-specified types (i.e., semantic specification) of data as per a given specified or selected (meta) protocol. Further, as per figures

2,3,5 the visual representation of said *disregarded data* (as well as 'regarded' data) would encompass the associated (*disregarded) data*), col. 8,lines 34-40, col. 9,lines 8-14,55-60) suggest such limitations;

16. Claim 13 ***additionally recites*** the limitations that "The system as recited in claim 10, wherein the set of semantic codes is a null set, and the at least one sensor is configured to use a default set of semantic codes.". The teachings of Maloney et al (col. 8,lines 19-26, col. 5,lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (*semantic (i.e., type)* of data, the actual data, and meta data levels, including active, initialized, default (i.e., null set specified), and degraded states (i.e., figure 3, 'promiscuous mode' reference), col. 8,lines 34-40, col. 9,lines 55-60) suggest such limitations;

17. Claim 14 ***additionally recites*** the limitations that "The system as recited in claim 1, wherein the analysis engine is located on a first host and an instance of the at least on,; sensor is located on a second host apart from the first host. ". The teachings of Maloney et al (figure 2, and associated description, col. 2,lines 15-33) suggest such limitations;

18. Claim 15 ***additionally recites*** the limitations that "The system as recited in claim, 14, comprising a second instance of the at least one sensor, wherein the second instance is located on a host apart from the second host.". The teachings of Maloney et al (figure 2, and associated description, col. 2,lines 15-33, col. 5,lines 34-38, col. 6,lines 33-38, col. 7,lines 22-24) suggest such limitations;

19. Claim 16 ***additionally recites*** the limitations that "The system as recited in claim 1, wherein the at least one sensor includes a sensor collector in communication with the analysis

engine.". The teachings of Maloney et al (col. 8,lines 19-26, col. 5,lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (data and meta data levels), and sensor routing of collection functions (i.e., figure 3), col. 8,lines 34-40, col. 9,lines 55-60) suggest such limitations;

20. Claim 17 ***additionally recites*** the limitations that "The system as recited in claim 1, further comprising a sensor collector disposed in a communication path between the analysis engine and the at least one sensor.". The teachings of Maloney et al (col. 8,lines 19-26, col. 5,lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (data and meta data levels), and sensor routing of collection functions (i.e., figure 3,configuration of *sensor manager*), col. 8,lines 34-40, col. 9,lines 55-60) suggest such limitations;

21. Claim 18 ***additionally recites*** the limitations that "The system as recited in claim 1, wherein the analysis engine is configured to load a rule set while the analysis engine is in operation.". The teachings of Maloney et al (col. 4,lines 20-33, col. 5,lines 7-17,33-53, col. 6,lines 45-59, col. 7,lines 7-34, col. 8,lines 34-50, col. 9,lines 9-14,37-41, col. 11,lines 1-5, col. 12,lines 21-34) suggest such limitations;

22. Claim 19 ***additionally recites*** the limitations that "The system as recited in claim 1, further comprising a second sensor, and wherein the analysis engine is configured to load a rule set for the second sensor while the analysis engine is in operation.". The teachings of Maloney et al (col. 4,lines 20-33, col. 5,lines 7-17,33-53, col. 6,lines 45-59, col. 7,lines 7-34, col. 8,lines

34-50, col. 9,lines 9-14,37-41, col. 11,lines 1-5, col. 12,lines 21-34, figure 2, and associated description, col. 2,lines 15-33, col. 6,lines 33-38) suggest such limitations;

23. Claim 20 ***additionally recites*** the limitations that "The system as recited in claim 19, wherein the rule set is configured to specify interactions of data from the second sensor with data from the at least one sensor.". The teachings of Maloney et al (col. 4,lines 20-33, col. 5,lines 7-17,33-53, col. 6,lines 45-59, col. 7,lines 7-34, col. 8,lines 34-50, col. 9,lines 9-14,37-41, col. 11,lines 1-5, col. 12,lines 21-34, figure 2, and associated description, col. 2,lines 15-33, col. 6,lines 33-38) suggest such limitations;

24. Claim 21 ***additionally recites*** the limitations that "The system as recited in claims 20, wherein the analysis engine is configured to ignore rules in the rule set that specify data not supplied by any sensor.". The teachings of Maloney et al (col. 4,lines 20-33, col. 5,lines 7-17,33-53, col. 6,lines 45-59, col. 7,lines 7-34, col. 8,lines 34-50, col. 9,lines 9-14,37-60, col. 11,lines 1-5, col. 12,lines 21-34, figure 2, and associated description, col. 2,lines 15-33, col. 6,lines 33-38,mmmm, col. 8,lines 19-26, col. 5,lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols, and *rules criteria* (data and meta data levels, including active, initialized, default (i.e., null set specified), and degraded states (i.e., figure 3, 'promiscuous mode' reference would encompass allowing data transfer and *the rules governing such transfer*, of specified and non-specified types (i.e., semantic specification) of data as per a given specified or selected (meta) protocol. Further, as per figures 2,3,5 the visual representation of said *disregarded data* (as well as 'regarded' data) would encompass the associated (*disregarded) data*)) suggest such limitations;

Conclusion

25. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100